



Your Social Security Number: Controlling the Key to Identity Theft

CONSUMER INFORMATION SHEET 4

▣ Your Social Security number is the key.

Originally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information.

With your SSN, an identity thief can get your credit history, your bank account, your charge accounts, and your utility accounts. A thief can also use the number to open new credit and bank accounts or to get a driver's license—all using your identity.

▣ Don't carry your Social Security card in your wallet.

You don't need to have your Social Security card with you at all times. Keep it at home in a safe place. Check for other cards that may have your SSN on them.

▣ Ask questions when they ask for your Social Security number.

There is no law that prevents businesses from asking for your SSN. And you may be denied service if you don't give the number. If giving your SSN to a business doesn't seem reasonable to you, ask if you can show another form of identification. Or ask if the business can use another number as your customer number.

Remember that some government agencies can require your SSN. These agencies include DMV, welfare offices, and tax agencies. Look for the required "disclosure" form. The form should state if giving the number is required or optional, how it will be used, and the agency's legal authority to ask for it.¹

▣ California law limits the public display of Social Security numbers.

A California law bars many organizations from publicly displaying SSNs.²

The law prohibits:

- Printing SSNs on ID cards or badges,
- Printing SSNs on documents mailed to customers, unless the law requires it or the document is a form or application,
- Printing SSNs on postcards or any other mailer where its visible without opening an envelope,



- Avoiding legal requirements by encoding or embedding SSNs in cards or documents, such as using a bar code, chip or magnetic strip,
- Requiring people to send SSNs over the Internet, unless the connection is secure or the number is encrypted, and
- Requiring people to use an SSN to log onto a web site, unless a password is also used.

The law applies to businesses, government and other entities.

▣ Ask your companies to change now.

Organizations may continue their current practices for using SSNs for existing customers, rather than stopping the practices barred by the new law described above—unless a customer requests otherwise in writing. You can ask a company or organization to treat your SSN as the law requires now. Send a letter that says something like the following: “I am hereby requesting that you comply with the requirements of California Civil Code section 1798.85 related to your use of my Social Security number. I understand that you have 30 days from the receipt of this letter to comply.”

IMPORTANT NOTE: Health care providers, health plans and insurance companies are given more time to comply with the ban on printing SSNs on ID cards. They must fully comply by July 2005.

▣ Getting a new Social Security number is probably not a good idea.

Victims of identity theft sometimes want to change their Social Security number. The Social Security Administration very rarely allows this. In fact, there are drawbacks to changing your number. It could result in losing your credit history, your academic records, and your professional degrees. The absence of any credit history under the new SSN would make it difficult for you to get credit, rent an apartment, or open a bank account.

▣ Here's where to get more information on Social Security numbers.

Identity Theft: If you think an identity thief is using your SSN, call the Social Security Fraud Hotline at 1-800-269-0271. If you think someone may be using your SSN to work, check your Social Security Personal Earnings and Benefit Statement. You can get a copy by calling 1-800-772-1213, or online at www.ssa.gov/online/ssa-7004.pdf. Also see the Social Security Administration's booklet “When Someone Misuses Your Number,” available at www.ssa.gov/pubs/10064.html.

What the Numbers Mean: For an explanation of the meaning of the numbers in SSNs, see “Structure of Social Security Numbers,” by Computer Professionals for Social Responsibility, available at www.cpsr.org/cpsr/privacy/ssn/ssn.structure.html.

More on Protecting Your SSN: “Fact Sheet 10: My Social Security Number: How Secure Is It?” by the Privacy Rights Clearinghouse, available at www.privacyrights.org/fs/fs10-ssn.htm.



Recommended Practices: For recommendations on how organizations can protect privacy in their handling of SSNs, see the Office of Privacy Protection's "Recommended Practices for Protecting the Confidentiality of Social Security Numbers," available on the Recommended Practices Web page at www.privacy.ca.gov. See also "Alternatives to Using Social Security Numbers in Large Organizations," at www.epic.org/privacy/ssn/alternatives_ssn.html.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. Readers desiring advice in particular cases should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the Office of Privacy Protection, California Department of Consumer Affairs, and (3) all copies are distributed free of charge.

NOTES

¹ The federal Privacy Act of 1974, 5 U.S. Code 552a, is available on the Privacy Laws Web page at <http://www.privacy.ca.gov/>.

² California Civil Code section 1798.85 can be found on the Office of Privacy Protection's Privacy Laws page at <http://www.privacy.ca.gov/>.